Global Cyber and Privacy Risks

A growing insurance solution marketplace

Presented by:
Eduard F. Goodman, J.D., LL.M., CIPP-US/C/E
Chief Privacy Officer
Identity Theft 911
Exponential Nature of Digital Technology

Moore’s Law
Nielsen’s Law
Kryder’s Law
Moore’s Law, 1966

"The number of transistors incorporated in a chip will approximately double every 24 months."

Gordon Moore, Intel co-founder
Moore’s Law

Decoding the human genome originally took 10 years to process; now it can be achieved in one week.
Nielsen’s Law, 1998/2008

"Network connection speeds for high-end home users would increase 50% per year, or double every 21 months"

Jakob Nielsen, Web Usability Consultant

Chart Source: http://www.nngroup.com/articles/law-of-bandwidth/
Kryder’s Law, 2005

“Storage capacity doubles every twelve months.”

Mark Kryder, SVP Research/CTO, Seagate Corp

How far have we come?

OSBORNE 1
- 4MHz CPU (Zilog Z80)
  - Weighs 100X more
  - 500X larger
- 64 KB of Memory
  - ‘Executive’ had 124 KB
- Screen - 5-inch, 52 character x 24 line monochrome CRT
- Available 300 baud modem
  - Equal to 0.002197266 Mbps
    - Avg. WiFi speed is 24-36 Mbps
- 11 software options

iPhone 4/5
- 412 MHz CPU (ARM11)
  - 100X CPU clock speed
- 64 GB of Memory or
  - 68,719,476,736 KB
- Costs 10X less (adjusted)
- Screen- 4-inch, 640 x 1136 pixel, 326ppi, 16,777,216 color touch screen
- WiFi, Bluetooth, 4G LTE
- 700,000 Apps as of 9/12
- Also includes:
  - Camera (still/video)
  - Audio Play/Record
  - Integrated GPS
  - Etc.
2.5 quintillion bytes of data created EVERY day

90% of the data in the world today has been created in the last 2 years

Graphic Source: http://www.domo.com/blog/2012/06/how-much-data-is-created-every-minute/

3,716
Breaches made public (min)

607,611,003
Records containing personal/private info of U.S. citizens and residents

Source: http://www.privacyrights.org/data-breach/new
Cyber Attack and Breach Risks

- 75% of attacks were “opportunistic” rather than “targeted”
- 78% of attacks were considered in the low to very low ‘difficulty level’
- 66% of breaches go undiscovered for months, or more
- 69% were discovered by someone OTHER than the party impacted

Source: www.verizonenterprise.com/DBIR/2013/
Reported Data Breach Incidents

Source: Open Security Foundation/DataLossDB.org
2012 Reported Breaches by Industry

Source: Open Security Foundation/DataLossDB.org
2012 Reported Breaches by Type

Source: Open Security Foundation/DataLossDB.org

- Hacking: 57%
- Fraud: 9%
- Stolen Laptop/Computer: 7%
- Web: 5%
- Unknown: 4%
- Document Disposal: 3%
- Stolen Document: 3%
- Snail Mail: 2%
- Email: 2%
- Other: 8%
2012 Reported Breaches by Vector

- **Outside**: 72%
- **Inside, Accidental**: 11%
- **Inside, Malicious**: 9%
- **Inside**: 4%
- **Unknown**: 4%

Source: Open Security Foundation / DataLossDB.org
2012 Breaches by Geography

- Data loss incidents per headquarter location

Source: Open Security Foundation / DataLossDB.org
Verizon 2013 Data Breach Investigations Report

- Of the 621 data breaches in this study, 92% were caused by outsiders

Source: Verizon, 2013 Data Breach Investigations Report
Verizon 2013 Data Breach Investigations Report

- Two-thirds of breaches in this report were considered opportunistic and not very difficult to execute.
- This indicates that the number of breaches could have been reduced or halted earlier through simple security measures and employee awareness and compliance.

### How do breaches occur?

- 52% used some form of hacking
- 76% of network intrusions exploited weak or stolen credentials
- 40% incorporated malware
- 35% involved physical attacks
- 29% leveraged social tactics
- 13% resulted from privilege misuse and abuse

### What commonalities exist?

- 75% driven by financial motives
- 71% targeted user devices
- 54% compromised servers
- 75% are considered opportunistic attacks
- 78% of initial intrusions rated as low difficulty
- 69% discovered by external parties
- 66% took months or more to discover

Source: Verizon, 2013 Data Breach Investigations Report
Annual Change Breach Causes

- Dramatic rise in hacking
- Unintended disclosure (presumably through employee error) is also rising, which is in opposition to the belief that we are more aware and that policies are maturing
- Breaches that originate from portable devices are trending lower
  - Hackers may be targeting servers more than portable devices
  - People are more reliant on personalized portable devices and may be more protective of those devices, which lowers loss

Source: Privacy Rights Clearinghouse
New Risk Vectors: Smart Phones

- Increase in smart phone based threats is staggering
- At the end of this 3Q13, the total number of samples in McAfee’s mobile malware “zoo” reached 50,926, with 28% of that arriving in 2013
- Malicious spyware combined with botnets are among the latest threats

Mobile Malware by Platform

Total Mobile Malware by Platform

Cost of Data Breach

- The Ponemon study represented 277 companies in 9 countries
- The 2012 consolidated average per capita cost of data breach for all country samples was $136
- Germany experienced the highest per capita cost at $199 and India was the lowest at $42 per compromised record

Source: Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis, May 2013
Cost of Data Breach

- US companies have the highest percentage of indirect cost and Brazil has the highest percentage direct cost.
- Direct expenses include forensic experts, hotline support, credit monitoring and discounts for future products and services.
- Indirect costs include in-house investigations and communication, lost customers and diminished acquisition rates.

Source: Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis, May 2013
Data Protection and Privacy as a global trade issue

• Privacy as a Right
• OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Key Principles for National Application):
  – Collection Limitation Principle
  – Data Quality Principle
  – Purpose Specification Principle
  – Use Limitation Principle
  – Security Safeguards Principle
  – Openness Principle
  – Accountability Principle
Mexico

• Federal Privacy Law:
  – Ley Federal de Protección de datos Personales en Posesión de los Particulares (Law on the Protection of Personal Data Held by Private Parties)
  – Went into effect July 5, 2010
  – Supervisory authority provided by the:
    • Instituto Federal de Acceso a la Información y Protección de Datos
    • (a.k.a. “the Institute for Access to Information and Data Protection”)
    • Lays out eight (8) core principles that data controllers must abide by
Mexico

- 8 core principles for data controllers to abide by under the regulation:
Regional Privacy Areas

- South America
  - Privacy regimes in force
  
  - Privacy regimes currently being considered

  Argentina
  Chile
  Peru
  Uruguay

  Brazil
  Bolivia
  Colombia